

Quantum Correlation Bounds for Quantum Information Experiments Optimization: the Wigner Inequality Case

F. A. Bovino*

Elsag Datamat

Via Puccini 2-16154 Genova (Italy)

I. P. Degiovanni†

Istituto Nazionale di Ricerca Metrologica

Strada delle Cacce 91-10135 Torino (Italy)

(Dated: February 15, 2008)

Violation of modified Wigner inequality by means binary bipartite quantum system allows the discrimination between the quantum world and the classical local-realistic one, and also ensures the security of Ekert-like quantum key distribution protocol. In this paper we study both theoretically and experimentally the bounds of quantum correlation associated to the modified Wigner's inequality finding the optimal experimental configuration for its maximal violation. We also extend this analysis to the implementation of Ekert's protocol.

PACS numbers: 03.65.Ud, 42.50.Ex, 03.67.Dd, 03.67.-a

The famous EPR paper [1] originated the debate on the existence of local-realistic hidden variables theory able to replace quantum theory. The Bohm's version of EPR argument [2] dealing with the quantum correlation of two-particle entangled state, triggered Bell's derivation of an experimentally testable inequality [3], in principle allowing the discrimination between the quantum world and the classical local-realistic one.

Since then, several Bell's inequalities using two or more particles have been proposed [4, 5, 6], and a lot of experiments with different quantum systems have been performed showing violation of Bell's inequality in good agreement with the predictions of quantum mechanics [6, 7, 8]. Furthermore the effect of practical inefficiencies has been studied [9], even if an experiment "ruling out" all the loopholes together has not yet been realized [6].

More recently, several studies on the *extension* of quantum correlation appeared, such as studies on the possibility of super-quantum correlation [10], on the relative extension of quantum correlations versus the classical ones [11], on the bounds of quantum correlation associated to Clauser-Horne-Shimony-Holt (CHSH) inequality [12, 13, 14].

On the other side, from the early days of quantum information it is clear that quantum correlation (entanglement), and Bell's inequality as mean to highlight its presence, has a central role in this new field. In this context, the most advanced application in quantum information is quantum key distribution (QKD) [15, 16], various systems of QKD have been implemented and tested by groups around the world [16]. In 1991 A. Ekert proposed a new QKD protocol whose security relies on the non-local behavior of quantum mechanics, i.e., on Bell's in-

equalities [17]. The firsts experimental implementations of Ekert's protocol were performed nine years later by Naik *et al.* [18] implementing a variant of this protocol based on CHSH inequality, and by Jennewein *et al.* [19] implementing a variant of this protocol based on the Wigner's inequality (WI).

In ref. [19] the violation of WI exploiting a two-photon singlet state was first proposed to provide an easier and equally reliable eavesdropping test. Unfortunately, this is not the case. We proved both theoretically and experimentally that if the eavesdropper has the control of both channels, he is able to violate WI with separable states [20, 21]. Furthermore we proposed a *modified* version of WI whose violation ensures the security of the communication [20, 21]. (Recently was brought to our attention Ref. [22], where the algebraic properties of the singlet state in connection with the original Wigner's inequality are investigated, arguing that the original Wigner's argument is not significant in deriving conclusions about local realism. It is noteworthy to observe that in the derivation of the modified WI there is not any assumption on the quantum state considered [20], thus Koc's considerations cannot be applied in the case of the modified WI).

Scope of this paper is to study theoretically and experimentally the bounds of quantum correlation associated to the modified WI, aiming not only to investigate the existence of super-quantum correlation, but mainly to find configuration for the maximal possible violation of modified WI, and for the optimal implementation of Ekert's QKD protocol based on this inequality.

We consider the operator \widehat{W} associated to the WI with a parametrization similar to the one proposed by Filipp and Svozil for the CHSH inequality [12, 13, 14]

$$\begin{aligned} \widehat{W} = & \widehat{P}_{+,A}(-\theta) \otimes \widehat{P}_{+,B}(0) + \widehat{P}_{+,A}(0) \otimes \widehat{P}_{+,B}(\theta) \\ & + \widehat{P}_{-,A}(0) \otimes \widehat{P}_{-,B}(0) - \widehat{P}_{+,A}(-\theta) \otimes \widehat{P}_{+,B}(\theta), \end{aligned} \quad (1)$$

where $\widehat{P}_{+,i}(\theta)$ is the projector on the state $|s_+(\theta)\rangle_i =$

*Electronic address: Fabio.Bovino@elsagdatamat.com

†Electronic address: i.degiovanni@inrim.it

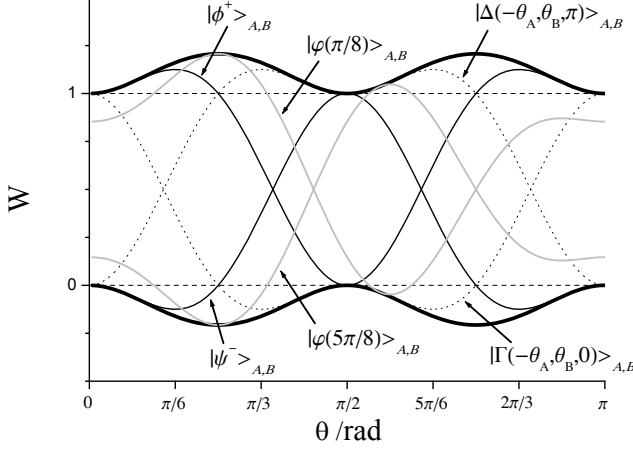


FIG. 1: Theoretical curves. Wigner's parameter classical correlation bounds are $W = 0$ and $W = 1$. Thick black lines are the minimum and maximum eigenvalues of the operator \widehat{W} (upper and lower bounds of quantum correlation). The maximal upper (lower) violation of WI can be achieved e.g. with $|\varphi(\pi/8)\rangle_{A,B}$ ($|\varphi(5\pi/8)\rangle_{A,B}$) (light gray lines). Curves corresponding to W obtained averaging on $|\psi^-\rangle_{A,B}$ and $|\phi^+\rangle_{A,B}$ (thin black line) and on $|\Gamma(-\theta_A, \theta_B, 0)\rangle_{A,B}$ and $|\Delta(-\theta_A, \theta_B, \pi)\rangle_{A,B}$ (dotted black line) are also shown.

$\cos(\theta)|H\rangle_i + \sin(\theta)|V\rangle_i$ of the i -th subsystem (with $i = A, B$), and $\widehat{P}_{-,i}(\theta)$ is the projector on the orthogonal state $|s_-(\theta)\rangle_i = \cos(\theta)|V\rangle_i - \sin(\theta)|H\rangle_i$.

Thus, the modified Wigner's parameter defined in [20, 21] is obtained as $W = \text{Tr}(\widehat{W} \widehat{\rho})$, with $\widehat{\rho}$ being the density matrix of our quantum system. Thus, we obtain the expression for W in Filipp-Svozil parametrization analogous to the one of [20, 21]

$$W = p_{-\theta_A, 0_B}(+A, +B) + p_{0_A, \theta_B}(+A, +B) + p_{0_A, 0_B}(-A, -B) - p_{-\theta_A, \theta_B}(+A, +B), \quad (2)$$

with $p_{\alpha_A, \beta_B}(\pm A, \pm B) = \text{Tr}[\widehat{P}_{\pm, A}(\alpha) \otimes \widehat{P}_{\pm, B}(\beta) \widehat{\rho}]$.

As discussed in [20, 21] the classical limit for the modified WI is $W \geq 0$, while the maximum violation obtainable with the singlet state $|\psi^-\rangle_{A,B} = 2^{-1/2}(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B)$ is $W = -0.125$ obtained when $\theta = \pi/6$. We also showed that the violation of $W \geq 0$ guarantees the security of the Ekert's protocol based on the modified WI.

To study the bounds of quantum correlation for the modified WI we exploited the *min/max* principle. In Fig. 1 we plot the minimum and the maximum eigenvalues of the operator \widehat{W} in Eq. (1) (black thick lines), while the other two eigenvalues do not violate the bound of classical correlation. The first observation is that \widehat{W} presents both an upper and lower bounds, and that the singlet state is not the one producing the maximal violation. In fact the

extremal values for the modified WI are -0.20711 and 1.20711 obtained for e.g. $\theta = \pi/4$.

The presence of the quantum correlation upper bound for WI leaded us to investigate on the existence of an upper bound also for classical correlation. With this aim we reconsider the Wigner's argument [4, 20]. The assumptions on locality and realism in the derivation of the (modified) WI are embedded in the classical probability distribution, $\mathcal{P}(x_1, x_2; y_2, y_3)$, where x_1 and x_2 are the hidden variables associated with the physical property inducing Alice's outcomes associated to the projection on $|s_{x_1}(-\theta)\rangle_A$ and $|s_{x_2}(0)\rangle_A$ respectively. Analogously y_2 and y_3 correspond to the physical property inducing Bob's outcomes associated to the projection on $|s_{y_2}(0)\rangle_B$ and $|s_{y_3}(\theta)\rangle_B$. Thus, we identify the possible values of $x_{1,2}$ and $y_{2,3}$ with Alice and Bob's measurement outcomes, in other words $x_{1,2} = +A, -A$ and $y_{2,3} = +B, -B$. Following this approach we write,

$$\begin{aligned} p_{-\theta_A, 0_B}(+A, +B) &= \sum_{x_2, y_3} \mathcal{P}(+A, x_2; +B, y_3), \\ p_{0_A, \theta_B}(+A, +B) &= \sum_{x_1, y_2} \mathcal{P}(x_1, +A; y_2, +B), \\ p_{-\theta_A, \theta_B}(+A, +B) &= \sum_{x_2, y_2} \mathcal{P}(+A, x_2; y_2, +B), \\ p_{0_A, 0_B}(-A, -B) &= \sum_{x_1, y_3} \mathcal{P}(x_1, -A; -B, y_2). \end{aligned} \quad (3)$$

Substituting Eq.s (3) in Eq. (2) we obtain

$$\begin{aligned} W &= \mathcal{P}(+A, +A; +B, +B) + \mathcal{P}(+A, +A; +B, -B) \\ &\quad + \mathcal{P}(-A, +A; +B, +B) + \mathcal{P}(+A, -A; +B, -B) \\ &\quad + \mathcal{P}(-A, +A; -B, +B) + \mathcal{P}(+A, -A; -B, -B) \\ &\quad + \mathcal{P}(-A, -A; -B, +B) + \mathcal{P}(-A, -A; -B, -B) \leq 1 \end{aligned}$$

where the last inequality is obtained by exploiting the normalization condition $\sum_{x_1, x_2, y_2, y_3} \mathcal{P}(x_1, x_2, y_2, y_3) = 1$. This is to our knowledge the first derivation of the upper bound of classical correlation associated to the (modified) WI.

Summarizing the Wigner's parameter bounds associated to local-realistic theory are $0 \leq W \leq 1$, while the bounds of quantum correlations in Filipp-Svozil parametrization are $-0.20711 \leq W \leq 1.20711$ at specific choices of the angle θ . Furthermore the states producing the maximal violation of the inequality $0 \leq W \leq 1$ for the upper (lower) bound is given by the eigenstate corresponding to the maximum (minimum) eigenvalue of \widehat{W} , and in none of these two cases it corresponds to the singlet state used in previous experiment [8]. In particular, the eigenstates corresponding to the maximum and the minimum eigenvalues of modified WI are of the form

$$\begin{aligned} |\varphi(\xi)\rangle_{A,B} &= \cos(\xi)|\phi^+\rangle_{A,B} + \sin(\xi)|\psi^-\rangle_{A,B} = \\ &= \frac{1}{\sqrt{2}}(|H\rangle_A|s_+(\xi)\rangle_B - |V\rangle_A|s_-(\xi)\rangle_B) \end{aligned} \quad (4)$$

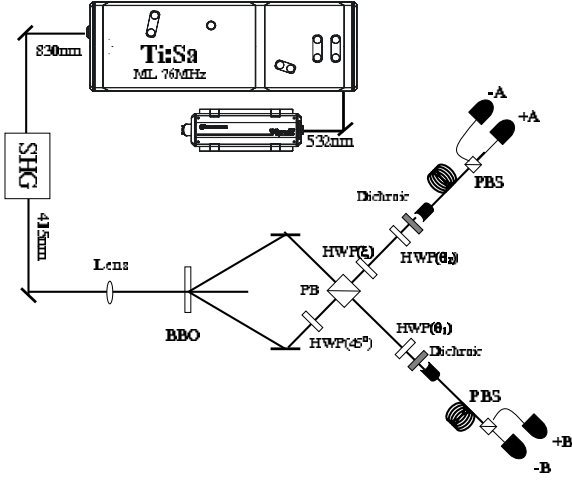


FIG. 2: Experimental setup.

with $|\phi^{(+)}\rangle_{A,B} = 2^{-1/2}(|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B)$. For example, in the case of $\theta = \pi/4$ the maximal violation of the upper bound is obtained when $\xi = \pi/8$ (upper light gray line in Fig. 1), while the maximal violation of lower bound is obtained when $\xi = 5\pi/8$ (lower light gray line in Fig.1).

According to the theoretical arguments discussed above it is of straightforward interest to perform an experiment to test the behavior of the quantum correlations for the modified WI. We perform this experiment exploiting the optical setup presented in Fig. 2, and analogous to the one we used in Ref. [14]. The source of pulsed parametric down-conversion (PDC) is obtained by a 3 mm length BBO nonlinear crystal pumped with ultra-short pump pulses (160 fs) at 415 nm generated from the second harmonic of a mode-locked Ti-Sapphire with repetition rate of 76 MHz. PDC degenerate photon pairs at 830 nm are generated by a non-collinear type II phase matching, providing eventually a polarization entanglement, i.e. the singlet state $|\psi^-\rangle_{A,B}$ [23], when time-compensated PDC scheme is applied [24]. To realize the set of entangled states $|\varphi(\xi)\rangle_{A,B}$ in Eq. (4) an half-wave plate (HWP) on the channel B is used to rotate the polarization of photon B .

The local measurements on photon A and B are performed by identical apparatuses composed of open-air fiber couplers collecting the PDC in single-mode optical fibers. HWPs before the fiber coupler together with fiber-integrated polarizing beam splitters (PBSs) and fiber polarization controllers project photons in the polarization basis. Photons at the output ports of the PBSs are detected by fiber coupled commercial photon counters. Dichroic mirror are placed in front of the fiber couplers to reduce stray-light. Coincident counts are measured by a non-commercial prototype of four-channel coincident circuit. Single-counts and coincidences are counted by a sixteen channels counter plug-in PC card.

Fig. 3 shows highly stable and repeatable W mea-

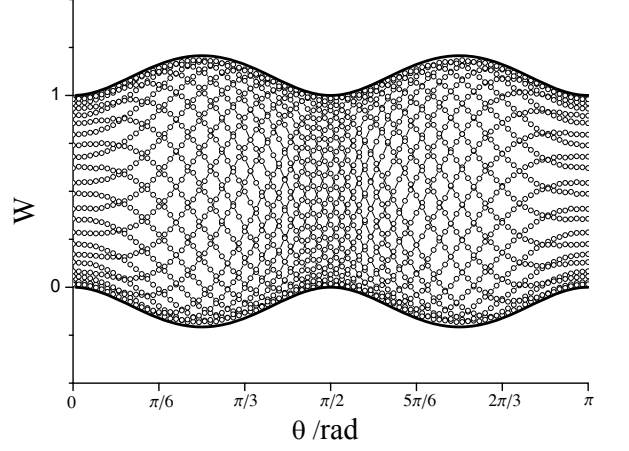


FIG. 3: Experimental results. Each dot corresponds to an experimental measurement of ${}_{A,B}\langle\varphi(\xi)|\widehat{W}|\varphi(\xi)\rangle_{A,B}$ performed with a different value of θ and ξ . Each curve corresponds to a fixed value of ξ . Theoretical upper and lower W bounds of quantum correlation are also shown (thick black lines).

surement points (dots) plotted versus θ , and the various curves are associated to different values of the parameter ξ . The thicker curves correspond to the theoretically predicted W quantum correlation bounds. There is a good qualitative and quantitative agreement between theoretical and experimental bounds, even if the experimental upper (lower) bounds stands slightly below (above) the theoretical predictions. These effects are, as usual, imputable to noise and imperfections associated to the polarization preservation and measurement of some setup components, namely HWPs, PBSs, and fibers. In fact, the discrepancy between the theoretical and the experimental results observed is confirmed by an equivalent noise level as verified during the alignment process, e.g. at specific angle settings of the polarizers [9]. Fig. 4 shows the contour plot corresponding to the experimental data in Fig. 3. This plot highlights the region of values of ξ and θ where we observed violations of both upper and lower bounds of the modified WI.

Let us now consider the problem of Ekert's protocol based QKD. According to Ref.s [17, 18, 19, 20], at least one of the measurement settings of the Ekert's protocol should produce binary non-local deterministic outputs, but local random outputs. In general the state producing the maximal violation of the WI are not suitable for QKD. Considering the four settings of the Wigner's protocol $\mathcal{S} = (\{-\theta_A, 0_B\}, \{-\theta_A, \theta_B\}, \{0_A, 0_B\}, \{0_A, \theta_B\})$,

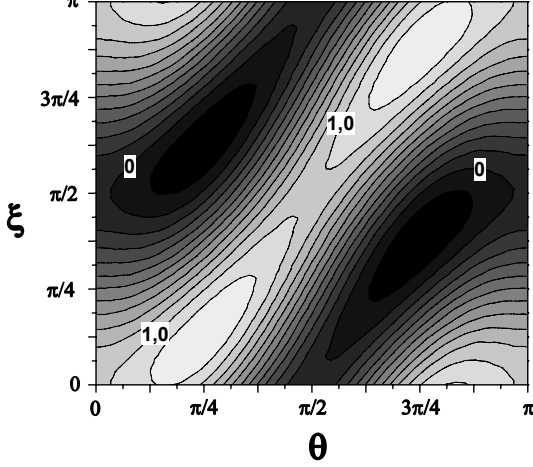


FIG. 4: Contour plot obtained from the experimental data in Fig. 3.

the states suitable for QKD should be of the form

$$\begin{aligned}
 |\Gamma(\alpha_A, \beta_B, \gamma)\rangle_{A,B} &= \frac{1}{\sqrt{2}}(|s_+(\alpha)\rangle_A |s_+(\beta)\rangle_B \\
 &\quad + e^{i\gamma} |s_-(\alpha)\rangle_A |s_-(\beta)\rangle_B), \\
 |\Delta(\alpha_A, \beta_B, \delta)\rangle_{A,B} &= \frac{1}{\sqrt{2}}(|s_+(\alpha)\rangle_A |s_-(\beta)\rangle_B \\
 &\quad + e^{i\delta} |s_-(\alpha)\rangle_A |s_+(\beta)\rangle_B) \quad (5)
 \end{aligned}$$

with $\{\alpha_A, \beta_B\} \in \mathcal{S}$.

In the case of measurement settings $\{-\theta_A, 0_B\}$, $\{0_A, \theta_B\}$, for any value of θ , γ and δ , the states in Eq. (5) do not produce any violation of WI, i.e. the states $|\Gamma(-\theta_A, 0_B, \gamma)\rangle_{A,B}$, $|\Delta(-\theta_A, 0_B, \delta)\rangle_{A,B}$ and $|\Gamma(0_A, \theta_B, \gamma)\rangle_{A,B}$, $|\Delta(0_A, \theta_B, \delta)\rangle_{A,B}$ are not suitable to guarantee the security of the Ekert's QKD protocol based on WI. By contrary violations of WI are observed for settings $\{0_A, 0_B\}$, $\{-\theta_A, \theta_B\}$.

In the case of setting $\{0_A, 0_B\}$ the maximal violation of the lower bound achievable is $W = -0.125$, obtainable with the state $|\Delta(0_A, 0_B, \pi)\rangle_{A,B}$, corresponding to the singlet state $|\psi^-\rangle_{A,B}$ when $\theta = \pi/6$ or $5\pi/6$ (lower thin black line in Fig. 1). Furthermore, at the same angles the maximal violation of the upper bound achievable with this setting ($W = 1.125$) are predicted. The state producing these violations is $|\Gamma(0_A, 0_B, 0)\rangle_{A,B}$, corresponding to the triplet state $|\phi^+\rangle_{A,B}$ (upper thin black line in Fig. 1).

Analogously, for setting $\{-\theta_A, \theta_B\}$ the maximal violation of the lower bound ($W = -0.125$) is observed for the state $|\Gamma(-\theta_A, \theta_B, 0)\rangle_{A,B}$ when $\theta = \pi/3$ or $2\pi/3$ (lower dotted black line in Fig. 1), while at the same angle the maximal violation of the upper bound ($W = 1.125$) is predicted for the state $|\Delta(-\theta_A, \theta_B, \pi)\rangle_{A,B}$ (upper dotted black line in Fig. 1).

This means that, in principle, there is not any advantage in using a state different from the singlet state to implement the Ekert's QKD protocol based on WI, or, equivalently, that the singlet state naturally produced by type II PDC is one of the optimal state for realizing QKD experiment with this protocol.

The last part of the paper is devoted to consider a more general parametrization for WI. Let us consider the Wigner's operator

$$\begin{aligned}
 \widehat{\mathcal{W}} &= \widehat{P}_{+,A}(\alpha) \otimes \widehat{P}_{+,B}(0) + \widehat{P}_{+,A}(0) \otimes \widehat{P}_{+,B}(\beta) \\
 &\quad + \widehat{P}_{-,A}(0) \otimes \widehat{P}_{-,B}(0) - \widehat{P}_{+,A}(\alpha) \otimes \widehat{P}_{+,B}(\beta), \quad (6)
 \end{aligned}$$

which is a generalization of the one in Eq. (1).

As the Wigner's parameter consists of independent local projection measurements on both Alice and Bob side, it's obvious that, by a proper rotation of the Poincaré's sphere at each side, any possible choice of these projections measurements can be reduced to the ones of the Eq. (6). Thus, the most general parametrization of the Wigner's parameter is equivalent to the one in Eq. (6).

By the application of the *min/max* principle, the bounds of quantum correlation for \mathcal{W} ($\mathcal{W} = \text{Tr}[\widehat{\mathcal{W}} \widehat{\rho}]$) are $-0.20711 \leq \mathcal{W} \leq 1.20711$, as in the Filipp-Svozil parametrization. This means that the generalization of the Wigner's parameter does not provide any advantage in terms of increasing the region of quantum correlation.

Eventually, also in the case of Ekert's QKD protocol based on WI there is not any advantage in using the generalized version of the Wigner's parameter with respect to the Filipp-Svozil one. In fact, following the same line of thought developed in the case of the Filipp-Svozil parametrization, the maximal violation for lower and upper bound achievable by states suitable for QKD are -0.125 and 1.125 , respectively.

In conclusion, we investigated theoretically and experimentally the bounds of quantum correlation associated to the modified WI according to Filipp-Svozil parametrization. We obtained the configuration for the maximal violation of modified WI, which, surprisingly, is not reachable by the singlet state as it happens for CHSH inequality. Furthermore we extended our analysis to the implementation of the Ekert's QKD protocol based on WI, and we observed that, in this context, the singlet state allows the optimal implementation of the QKD protocol. Furthermore we proved that there is not any advantage in considering generalized parametrization with respect to the Filipp-Svozil one.

Acknowledgments

We wish to thank M. Genovese for helpful discussion and to bring to our attention Ref. [22]. ElSag Datamat carried out this work within the contract Ministero della Difesa n. 9223 del 22.12.2005 ECFET QAP-2005-015848.

-
- [1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
 - [2] D. Bohm, Phys. Rev. **108**, 1070 (1957).
 - [3] J. Bell, Physics **1**, 195 (1964).
 - [4] E. P. Wigner, Am. J. Phys **38**, 1005 (1970).
 - [5] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969), J. F. Clauser, and M. A. Horne, Phys. Rev. D **10**, 526 (1974), J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989), D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
 - [6] M. Genovese, Phys. Rep. **413**, 319 (2005); *and References therein*.
 - [7] A. Aspect J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982), Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988), Y. H. Shih, and C. O. Alley, Phys. Rev. Lett. **61**, 2921 (1988), J. G. Rarity, and P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990), P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **47**, R2472 (1993), W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998), M. A. Rowe *et al.*, Nature **409**, 791 (2001).
 - [8] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
 - [9] F. A. Bovino, G. Castagnoli, A. Cabello, and A. Lamas-Linares, Phys. Rev. A **73**, 062110 (2006).
 - [10] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
 - [11] A. Cabello, Phys. Rev. A **72**, 012113 (2005).
 - [12] A. Cabello, Phys. Rev. Lett. **92**, 060403 (2004).
 - [13] S. Filipp, and K. Svozil, Phys. Rev. A **69**, 032101 (2004).
 - [14] F. A. Bovino, G. Castagnoli, S. Castelletto, and I. P. Degiovanni, Phys. Rev. Lett. **92**, 060403 (2004).
 - [15] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, (IEEE, New York 1984), p. 175.
 - [16] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); M. Dusek, N. Lutkenhaus, M. Hendrych, Progress in Optics, **49**, 381 (2006); *and References therein*.
 - [17] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
 - [18] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
 - [19] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
 - [20] S. Castelletto, I. P. Degiovanni, and M. L. Rastello, Phys. Rev. A **67**, 044303 (2003).
 - [21] F. A. Bovino, A. M. Colla, G. Castagnoli, S. Castelletto, I. P. Degiovanni, and M. L. Rastello, Phys. Rev. A **68**, 034309 (2003).
 - [22] Y. Koc, Il Nuovo Cimento, **108**, 1115 (1993).
 - [23] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
 - [24] Y.-H. Kim, S. P. Kulik, M. V. Chekhova, W. P. Grice, and Y. Shih, Phys. Rev. A **67**, 010301(R) (2003).